



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,810	05/14/2001	Umesh Krishnaswamy	1014-001US01	2001

28863 7590 01/24/2006  
SHUMAKER & SIEFFERT, P. A.  
8425 SEASONS PARKWAY  
SUITE 105  
ST. PAUL, MN 55125

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/854,810

Applicant(s)

KRISHNASWAMY ET AL.

Examiner

Christopher A. Revak

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-9, 11-19 and 22-35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 5-9, 11-14, 19 and 22-25 is/are allowed.
- 6) ☒ Claim(s) 1-4, 15-18 and 26-35 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 5/14/01 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date. _____  | 6) <input type="checkbox"/> Other: _____                                    |

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments filed August 29, 2005 have been fully considered but they are not persuasive.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claims. The applicant has provided various examples of the limitations "software processes" and "interrupt service routines", however the functionality of the limitations argued by the applicant is not recited in the claims and the applicant's arguments are moot. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In regards to the applicant's arguments that Joyce fails to disclose of either "software processes" or "interrupt service routines", the examiner contends that the teachings of Joyce does recite of these limitations. The teachings of Joyce are based "software processes" using heuristics in a firewall that can learn from and adapt to data flowing through the firewall, see column 1, lines 34-36. "Interrupt service routines" is broadly interpreted by the examiner as a routine requiring attention when a particular situation arrives, namely upon receiving a specific rating based on a received packet in the teachings of Joyce whereby that packet is further processed. The examiner notes

that the claims recite of "software process" or "interrupt driven service routine" in the alternative form and the claim limitations only require one situation to be met, not both.

The applicant argues that Joyce fails to disclose " processing a packet based on the detection of an event or based on detection of a network attack". The examiner respectfully disagrees since Joyce recites that selective processing is performed using different rules in order to identify the network attack as indicated by the applicant. Joyce further discloses if a data packet is rated marginal confidence, it is released to the firewall for more complex processing and low confidence packets are subject for additional analysis to determine why it was classified that way, see column 2, lines 51-60. The received packet is determined to be suspect, or a potential network attack, as is taught by Joyce and the detection of this event leads to further analysis in the teachings of Joyce to determine the actual result.

With respect to claim 27, it is argued by the applicant that neither Joyce or Gleichauf et al fail to teach "rate-limiting operating mode" or a "counter for use in enabling such a mode". The examiner respectfully disagrees, Gleichauf et al does indeed disclose of controlling the usage rate of resources in order to process packets, see column 8, lines 27-32, 49-52, & 58-62. The teachings of Gleichauf et al recite of determining threshold which implies usage of a counter to determine the threshold value and if that value has exceeded the threshold.

With respect to claim 31, the applicant argues that the examiner states "a context switch is not used within the teachings of Gleichauf et al since it is not disclosed" and that the "Applicants are confused as to how the examiner rejected claim 31 based on

this admission.” There exists no antecedent basis for a context switch in dependent claims 30 and 31, or in independent claim 26 and since it is a negative limitation, the “context switch” is not used in the applicant’s claim language and it is not needed in the teachings of Gleichauf et al.

2. Applicant’s amendments and arguments with respect to claims 5-9,11-14,19, and 22-25 have been fully considered and are persuasive.
3. The objection to claim 35 is hereby withdrawn by the examiner.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4,15-18,26,28,29, and 33-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Joyce, U.S. Patent 6,519,703.

As per claims 1,15, and 26, Joyce discloses of a method for a firewall (routing device) that comprises a detection module to detect the presence of a network attack, a network interface to receive an inbound packet from the network, and a routing engine to selectively process the packet using a heuristic stage (software process/mode) or an interrupt driven service routine (mode) based on the detection of a network attack (col.

2, lines 30-57). The examiner is interpreting the interrupt driven service routine as being packets rated as "high confidence" and are released into the traditional firewall rule base for further processing, see column 2, lines 47-51.

As per claim 2, the teachings of Joyce disclose that the event comprises a network attack (col. 2, lines 57-60).

As per claim 3, Joyce discloses of invoking a service routine using a software interrupt when the event is not detected and invoking a software process using to initiate (via a wakeup signal) the further processing of a suspicious packet upon detection of the event (col. 2, lines 30-57).

As per claims 4 and 17, it is disclosed by Joyce of detecting the presence of an event comprises detecting the event based on a traffic level of inbound packets received by a firewall (router)(col. 3, lines 19-25 and col. 4, lines 35-39).

As per claim 16, Joyce teaches of selectively processing the packet using a heuristic stage (software process/mode) or an interrupt driven service routine (mode) based on the detection of a network attack (col. 2, lines 30-57).

As per claim 18, Joyce discloses that the detection module detects the presence of a denial of service attack (col. 4, lines 32-43).

As per claims 28 and 29, Joyce teaches of a network service module being invoked in response to a hardware interrupt from the network interface and a set of packet service routines to service inbound packets in accordance with a plurality of network protocols (col. 2, lines 30-57 and col. 3, lines 29-58). A service routine is invoked using a software interrupt when the event is not detected and invoking a

software process using to initiate (via a wakeup signal) the further processing of a suspicious packet (col. 2, lines 30-57).

As per claim 33, it is disclosed by Joyce of detecting the presence of an event comprises detecting the event based on a traffic level of inbound packets received by a firewall (router)(col. 3, lines 19-25 and col. 4, lines 35-39), wherein the event is a network attack (col. 2, lines 57-60).

As per claim 34, Joyce discloses that the detection module detects the presence of a denial of service attack (col. 4, lines 32-43).

As per claim 35, Joyce teaches of detecting the presence of an event comprises detecting the event based on a traffic level of inbound packets received by a firewall (router) in response to the interrupt (col. 3, lines 19-25 and col. 4, lines 35-39), wherein the event is a network attack (col. 2, lines 57-60). It is interpreted by the examiner that a pointer is selected from a table of pointers since it determines the mode of operation based on the severity of the packet rating.

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 27 and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Joyce, U.S. Patent 6,519,703 in view of Gleichauf et al, U.S. Patent 6,301,668.

As per claim 27, Joyce disclose of selectively process the packet using a heuristic stage (software process/mode) or an interrupt driven service routine (mode) based on the detection of a network attack (col. 2, lines 30-57). The teachings of Joyce are silent in disclosing of enabling a rate limiting operating mode when a threshold is exceeded. Gleichauf et al discloses of controlling the usage rate of computer resources to process traffic (packets)(col. 8, lines 27-32,49-52, & 58-62). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply means for controlling the usage rate of computer resources. Gleichauf et al discloses of motivation for the limiting of usage rates of computer resources by reciting system services can be prioritized based on the importance of the services and to be able to adapt to a changing network environment by maintaining a sufficient level of security (col. 3, lines 21-24 and col. 8, lines 49-56). It is obvious that the teachings of Joyce would have found the teachings of Gleichauf et al beneficial in the aspect of being able to maintain a sufficient level of security in a changing network environment.

As per claim 30, the teachings of Joyce disclose of selectively process the packet using a heuristic stage (software process/mode) or an interrupt driven service routine (mode) based on the detection of a network attack (col. 2, lines 30-57). The teachings of Joyce fail to disclose of a software process controlling the usage rate of computer resources to process packets. It is disclosed by Gleichauf et al of a software process controlling the usage rate of computer resources to process traffic (packets)(col. 8, lines 27-32,49-52, & 58-62). It would have been obvious to a person of ordinary skill in the



art at the time of the invention to have been motivated to apply means for controlling the usage rate of computer resources. Gleichauf et al discloses of motivation for the limiting of usage rates of computer resources by reciting system services can be prioritized based on the importance of the services and to be able to adapt to a changing network environment by maintaining a sufficient level of security (col. 3, lines 21-24 and col. 8, lines 49-56). It is obvious that the teachings of Joyce would have found the teachings of Gleichauf et al beneficial in the aspect of being able to maintain a sufficient level of security in a changing network environment.

As per claim 31, the teachings of Gleichauf et al disclose of a software process that controls the usage rate of computing resources by determining an execution period that the software process has executed and pausing execution of the software process for a sleep period when the execution period exceeds a threshold (col. 8, lines 27-32, 49-52, & 58-62). Please refer above for the motivational benefits of applying the teachings of Gleichauf et al to the teachings of Joyce. It is interpreted that a context switch is not used within the teachings of Gleichauf et al since it is not disclosed.

As per claim 32, Gleichauf et al discloses of the software process dynamically adjusting the sleep period during the network attack (col. 8, lines 27-32, 49-52, & 58-62). Please refer above for the motivational benefits of applying the teachings of Gleichauf et al to the teachings of Joyce.

***Allowable Subject Matter***

8. Claims 5-9, 11-14, 19, and 22-25 are allowed.

***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

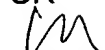
10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

  
January 21, 2006



Christopher Revak  
Primary Examiner  
AU 2131

1/21/06